ASA 8. 3: Установление подключения и устранение неполадок подключения через устройство обеспечения безопасности Cisco

Содержание

Введение

Когда устройство адаптивной защиты Cisco (ASA) первоначально настроено, это имеет стандартную политику безопасности, куда все на внутренней части могут выйти, и никто с внешней стороны не может войти. Если ваш узел требует другой политики безопасности, можно позволить внешним пользователям соединяться с Web-сервером через ASA.

Как только вы устанавливаете основное подключение через Cisco ASA, можно изменить конфигурацию межсетевого экрана. Удостоверьтесь любые изменения конфигурации, которые вы делаете к ASA, соответствуют вашей политике безопасности узла.

См. PIX/ASA: Установите и Подключение Устранения неполадок через Cisco Security Appliance для одинаковой конфигурации на Cisco ASA с версиями 8.2 и ранее.

Предварительные условия

Требования

Этот документ предполагает, что некоторые базовые конфигурации были уже завершены на Cisco ASA. См. эти документы для примеров начальной конфигурации ASA:

- ASA 8. 3 (x): подключите одиночную внутреннюю сеть с Интернетом
- Настройка PPPoE-клиент на устройстве адаптивной защиты Cisco (ASA)

Используемые компоненты

Сведения в этом документе основываются на устройстве адаптивной защиты Cisco (ASA), который выполняет версию 8.3 и позже.

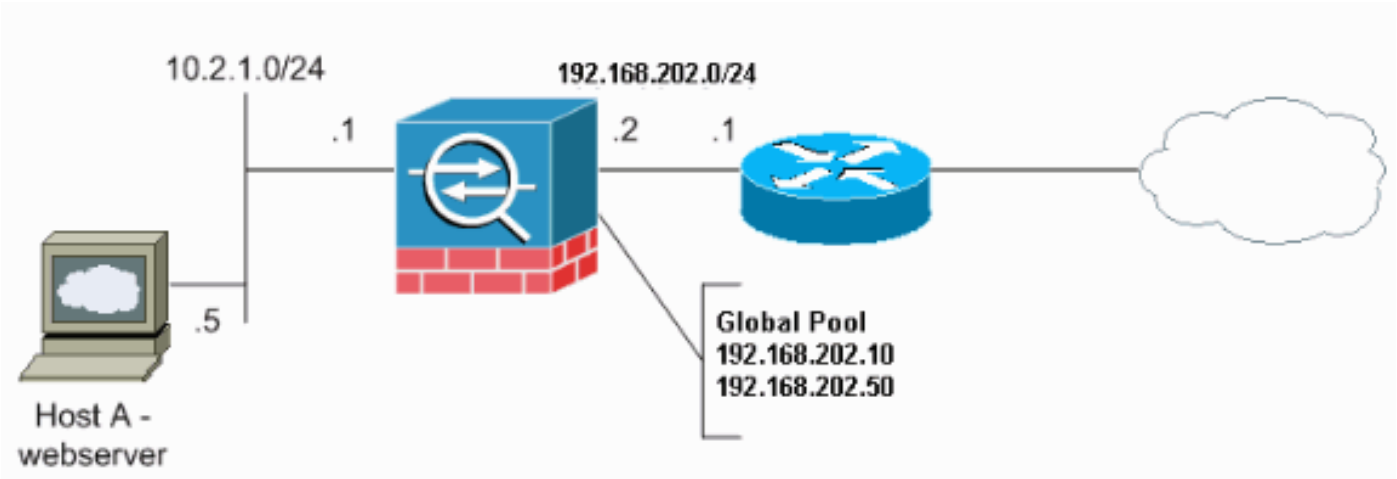
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Как работает подключение через ASA

В этой сети хост A – веб-сервер с внутренним адресом 10.2.1.5. Веб-серверу назначен внешний (транслированный) адрес – 192.168.202.5. Чтобы получить доступ к веб-серверу, пользователи Интернет должны указать этот адрес – 192.168.202.5. Данный адрес должен являться записью DNS для веб-сервера. Другие подключения из Интернета запрещены.



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Настройте подключение через Cisco ASA

Выполните эти шаги для настройки подключения через ASA:

1. Создайте сетевой объект, который определяет внутреннюю подсеть и другой сетевой объект для диапазона пула IP. Настройте NAT с помощью этих сетевых объектов:
   `object network inside-net subnet 0.0.0.0 0.0.0.0 object network outside-pat-pool range 192.168.202.10 192.168.202.50 nat (inside,outside) source dynamic inside-net outside-pat-`

```
pool
```

2. Назначьте статические транслированные адреса внутренним хостам, к которым пользователи Интернет имеют доступ.
```
object network obj-10.2.1.5 host 10.2.1.5 nat (inside,outside) static 192.168.202.5
```
3. Используйте **команду access-list**, чтобы позволить внешним пользователям через Cisco ASA. **Всегда используйте преобразованный адрес в команде access-list.**
```
access-list 101 permit tcp any host 192.168.202.5 eq www access-group 101 in interface outside
```

Разрешение широковещательного трафика ARP

Устройство защиты подключается к той же сети на внешних и внутренних интерфейсах. Поскольку межсетевой экран не является маршрутиризированнымом узел, можно легко представить прозрачный межсетевой экран существующей сети. Переназначение IP-адреса необязательно. Трафик IPv4 разрешается через прозрачный межсетевой экран автоматически (с более безопасного интерфейса на менее безопасный без использования списка доступа). Протоколы разрешения адресов (ARP) разрешены в обоих направлениях через прозрачный межсетевой экран без использования списка доступа. Проверка ARP-трафика осуществляется с помощью функции инспектирования ARP. Для трафика третьего уровня, который передается от менее безопасного к более безопасному интерфейсу, требуется расширенный список доступа.

Примечание: Прозрачный режим устройства защиты не передает CDP-пакеты или пакеты IPv6 либо пакеты, не имеющие допустимого значения EtherType, превышающего или равного 0x600. Например, невозможно прохождение пакетов IS-IS. Исключением является поддерживаемые блоки BPDU (Блок данных протокола моста).

Разрешенные MAC-адреса

Эти MAC-адреса получателей разрешены для прохождения трафика через прозрачный межсетевой экран. MAC-адреса не в этом списке отброшены:

- Реальный широковещательный MAC-адрес получателя, равный FFFF.FFFF.FFFF
- MAC-адреса групповой адресации IPv4 с 0100.5E00.0000 по 0100.5EFE.FFFF
- MAC-адреса групповой адресации IPv6 с 3333.0000.0000 по 3333.FFFF.FFFF
- Адрес групповой адресации BPDU, равный 0100.0CCC.CCCD
- Многоадресные MAC-адреса AppleTalk с 0900.0700.0000 по 0900.07FF.FFFF

Неразрешенный трафик режима маршрутизатора

В режиме маршрутизатора некоторым типам трафика не удается пройти через устройства защиты, даже если он разрешен в списке доступа. Однако прозрачный межсетевой экран, разрешает прохождение почти любому трафику с помощью расширенного списка доступа (для IP-трафика) или списка доступа EtherType (для не IP-трафика).

Например, с помощью прозрачного межсетевого экрана можно установить смежности протокола маршрутизации. Можно разрешить прохождение трафика, основанного на расширенном списке доступа таких протоколов, как протокол предпочтения кратчайшего пути (OSPF), протокол маршрутной информации (RIP), усовершенствованный внутренний протокол маршрутизации сетевых интерфейсов (EIGRP) или протокол пограничных шлюзов (BGP). Точно так же протоколы, такие как Протокол HSRP или Протокол VRRP могут пройти

через устройство безопасности.

Не IP-трафик (например, AppleTalk, IPX, BPDUs, и MPLS) может быть настроен на прохождение с помощью списка доступа EtherType.

Если какие-либо функции не поддерживаются прозрачным межсетевым экраном, можно разрешить прохождение трафика через него, чтобы вышестоящие или нижестоящие маршрутизаторы смогли обеспечить необходимую функциональность. Например, при помощи расширенного списка доступа, можно позволить трафик Протокола DHCP (динамического конфигурирования узла) (вместо неподдерживаемой Характеристики ретрансляции DHCP) или многоадресный трафик, такой как созданный IP/TV.

Устранение неполадок соединения

Если пользователям Интернет не удалось получить доступ к веб-узлу, необходимо выполнить следующие действия:

1. Убедитесь, что введенная настройка адресов верна:Допустимый внешний адресПравильный внутренний адресВнешняя DNS имеет транслированный адрес
2. Проверьте внешний интерфейс на наличие ошибок.Устройство обеспечения безопасности Cisco предварительно настроено для автоматического определения скорости и дуплексных режимов интерфейса. Однако существуют некоторые ситуации, которые могут вызвать сбой процесса автоматического согласования. Это результат несоответствия значений скорости или дуплексного режима (а также падение производительности). Для критически важной сетевой инфраструктуры, Cisco аппаратно программирует скорость и дуплексный режим на каждом интерфейсе, так что вероятность возникновения ошибок минимальна. Эти устройства обычно не перемещаются. Поэтому при настройке их должным образом вы не должны должны быть изменять их.**Пример:**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex full asa(config-if)#speed 100 asa(config-if)#exit` В некоторых ситуациях, аппаратное программирование скорости и дуплексного режима приводит к формированию ошибок. Поэтому необходимо настроить интерфейс к настройке по умолчанию режима автоматического опознавания как показано в примере:**Пример:**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex auto asa(config-if)#speed auto asa(config-if)#exit`
3. Если трафик не передает или получает через интерфейс ASA или маршрутизатора головной станции, попытайтесь очистить статистику ARP.`asa#clear arp`
4. Используйте **объект show run** и **команды show run static**, чтобы удостовериться, что включено статическое преобразование.**Пример:**
   `object service www service tcp source eq www object network 192.168.202.2 host 192.168.202.2 object network 10.2.1.5 host 10.2.1.5 object service 1025 service tcp source eq 1025 nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www` В этом сценарии, внешний IP-адрес используется для отображения IP-адреса для веб-сервера.
   `nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www`
5. Проверьте, чтобы видеть, что маршрут по умолчанию на Web-сервере указывает к внутреннему интерфейсу ASA.
6. Проверьте таблицу преобразования, используя команду show xlate, чтобы увидеть, было ли создано преобразование.
7. Используйте команду logging buffered для проверки файлов журнала, чтобы видеть,

запрещает ли, происходят. (Проверьте наличие преобразованных адресов и посмотрите есть ли какие-либо отказы.).)

8. Используйте команду перехвата:
   `access-list webtraffic permit tcp any host 192.168.202.5 capture capture1 access-list webtraffic interface outside` **Примечание:** Данная команда создает большой объем выходных данных. Это может привести к зависанию или перезагрузке маршрутизатора при большом объеме трафика.
9. Если пакеты добираются до ASA, удостоверьтесь, что ваш маршрут на Web-сервер от ASA корректен. (Проверьте команды маршрута в своей конфигурации ASA.)
10. Проверьте, отключен ли прокси-ARP. Выполните команду show running-config sysopt в ASA 8.3.3Здесь, прокси - протокол преобразования адресов отключен **командой sysopt noproxyarp outside**:`ciscoasa#show running-config sysopt no sysopt connection timewait sysopt connection tcpmss 1380 sysopt connection tcpmss minimum 0 no sysopt nodnsalias inbound no sysopt nodnsalias outbound no sysopt radius ignore-secret sysopt noproxyarp outside sysopt connection permit-vpn` Чтобы включить заново прокси-ARP, введите данную команду в режиме глобального конфигурирования:`ciscoasa(config)#no sysopt noproxyarp outside` Когда хост посылает IP-трафик другому устройству в той же сети Ethernet, этому хосту необходимо знать MAC-адрес устройства. ARP — протокол 2 уровня, который определяет IP-адрес для MAC-адреса. Хост посылает ARP-запрос "Кто владеет данным IP-адресом?"?". Устройство, которое обладает данным IP-адресом, отвечает "Мой IP-адрес; вот мой MAC-адрес."."Прокси-ARP позволяет устройствам защиты отвечать на запрос ARP от имени хостов, находящихся за ним. Это происходит путем посылки ответов на запросы ARP для статически назначенных адресов этих узлов. Устройство безопасности отвечает на запрос со своим собственным MAC-адресом, затем передает пакеты IP к соответствующему внутреннему хосту.Например, на схеме в данном документе показано, что когда запрос ARP делается для глобального IP-адреса веб-сервера, 192.168.202.5, устройство защиты выдает в ответ собственный MAC-адрес. Если прокси - протокол преобразования адресов не включен в этой ситуации, хосты на внешней сети устройства безопасности не могут достигнуть Web-сервера путем запуска запроса ARP для адреса 192.168.202.5. Дополнительную информацию о команде sysopt см. в справочнике по командам.
11. В случае, когда все настроено правильно, а пользователю все равно не удается получить доступ к веб-серверу, обратитесь в Техническую поддержку Cisco.

Сообщение об ошибках - %ASA-4-407001:

Несколько хостов не могут соединиться с Интернетом, и сообщение об ошибках `Error Message - %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded` получено в системном журнале. Как решена эта ошибка?

Когда количество пользователей превышает пользовательский предел используемой лицензии, это сообщение об ошибках получено. Для решения этой ошибки обновите лицензию на более высокое количество пользователей. Это может быть 50, 100, или лицензия неограниченного пользователя как требуется.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES

- Уведомления о дефекте для специалистов по продуктам безопасности (включая устройство адаптивной защиты Cisco (ASA))
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация